

An Intuitive Hamiltonian for Quantum Search

Stephen Fenner*

Department of Computer Science and Engineering

University of South Carolina

CSE-TR-2000-1

April 24, 2000

Abstract

We present new intuition behind Grover’s quantum search algorithm by means of a Hamiltonian. Given a black-box Boolean function $f : \{0, 1\}^n \rightarrow \{0, 1\}$ such that $f(w) = 1$ for exactly one $w \in \{0, 1\}^n$, Grover [4] describes a quantum algorithm that finds w in $O(2^{n/2})$ time. Farhi & Gutmann [3] show that w can also be found in the same amount time by letting the quantum system evolve according to a simple Hamiltonian depending only on f . Their system evolves along a path far from that taken by Grover’s original algorithm, however. The current paper presents an equally simple Hamiltonian matching Grover’s algorithm step for step. The new Hamiltonian is similar in appearance from that of Farhi & Gutmann, but has some important differences, and provides new intuition for Grover’s algorithm itself. This intuition both contrasts with and supplements other explanations of Grover’s algorithm as a rotation in two dimensions, and suggests that the Hamiltonian-based approach to quantum algorithms can provide a useful heuristic for discovering new quantum algorithms.

1 Introduction

Quantum algorithms can, in theory at least, solve useful problems faster than classical algorithms. Two primary families of quantum algorithms in this regard are algorithms for factoring and discrete log [9], and Grover’s search algorithms with quadratic speed-up [4, 5].

There are many variations on Grover’s original algorithm—counting, starting with partial data, multiple targets, et cetera. The algorithm is also surprisingly robust; although the original algorithm uses the Walsh-Hadamard transform, essentially any unitary operator will do just as well []. Starting with a simple condition on what transform is used, we will show how Grover’s algorithm arises from a particularly simple—almost naive—intuition about quantum algorithms. Our ideas also generalize to variants of Grover’s algorithm.

There have been good explanations in the literature [5, 8] of how and why fast quantum search works: the initial state is slowly rotated (in two complex dimensions) into the target state by repeatedly applying a special operator known as Grover’s iterate. Using a more physics-based approach, Farhi & Gutmann [3] describe an “analog” version of quantum search by means of a simple, time-independent Hamiltonian which transforms any initial state $|\sigma\rangle$ into some prespecified target state $|w\rangle$ in optimal time, provided that $|\sigma\rangle$ and $|w\rangle$ are not orthogonal. Their analog algorithm rotates the initial state into the target state in the same time that Grover’s “digital”

*Supported in part by NSF Grant CCR-9996310. Email fenner@cs.sc.edu.

algorithm does, yet their rotation strays far from the intermediate states reached in the original algorithm by applying Grover's iterate.

We show here that a simple, time-independent Hamiltonian for a system of qubits results in time evolution matching Grover's iterate exactly. This Hamiltonian also provides a nice, simple insight into the workings of the algorithm that is new, to the best of our knowledge.

Our Hamiltonian bears some resemblance to that of Farhi & Gutmann, although ours was conceived independently. Ours differs from theirs in important respects, however, and may not be as plausible physically, but it does closely coincide with the iterations of Grover's algorithm, and thus gives a much closer simulation of a digital quantum circuit by an analog process and vice versa. While Farhi & Gutmann's Hamiltonian is appealing from a physical point of view, ours is appealing from an algorithmic perspective. The heuristic it gives for Grover's algorithm suggests that other digital quantum algorithms might be found by first looking at analog versions. (More work on analog algorithms has been done recently, see [2] for example.)

1.1 Structure of the Paper

We give mathematical preliminaries in Section 2, including a brief description of Grover's algorithm as described in [5]. In Section 3 we show how Grover's algorithm arises from a simple-minded approach to quantum search. The operator we describe there corresponds directly to our Hamiltonian, which in Section 4 we compare with that of Farhi and Gutmann [3], and show how it generates Grover's iterate. Most of our work was done independently of [3] before it came to our attention, so our approach to the problem is different. In Section 5, we suggest a Hamiltonian-based approach to quantum algorithms in general, and we present open problems.

2 Preliminaries

We work with linear operators over a fixed N -dimensional Hilbert space. A standard norm on operators is defined as

$$|A| = \sup_{|v|=1} |Av|,$$

where A is an operator and $|\cdot|$ on the right hand side is the standard hermitian norm on the Hilbert space. This norm on operators satisfies $|AB| \leq |A| \cdot |B|$. Clearly, all unitary operators have unit norm. The exponential map on operators is defined as

$$e^A = I + A + \frac{A^2}{2!} + \frac{A^3}{3!} + \cdots, \quad (1)$$

where I is the identity operator.

If A is skew hermitian ($A^\dagger = -A$), then e^A is unitary. Conversely, for any unitary U there is a skew hermitian A such that $U = e^A$. As in the case with the exponential function on scalars, we also have

$$e^A = \lim_{k \rightarrow \infty} \left(I + \frac{A}{k} \right)^k. \quad (2)$$

For an n -qubit system we assume the standard basis of states $|i\rangle$ indexed by classical bit configurations $i \in \{0, 1\}^n$. We use lower-case Roman letters to label basis states, and lower-case Greek letters to label other (arbitrary) states in the Hilbert space.

2.1 Grover's Search Algorithm

Here we briefly review Grover's search algorithm. Fix an integer n and let $N = 2^n$. Let f be a Boolean-valued function on n -bit strings such that $f(w) = 1$ for exactly one w (the *target*), $0 \leq w < N$ (identifying strings with integers). A simple version of Grover's algorithm is to find w via a quantum algorithm where inputs to f are stored in n qubits, and f is available as a black box function (oracle) that can be queried by the algorithm. Alternately, we may assume that $f(y)$ is efficiently computable given y , and embed the computation of f into the quantum circuit.

In this setting, Grover's algorithm (as described in [5, 6] or [7]) uses three n -qubit unitary transforms:

1. an arbitrary, easy-to-compute U such that $\langle w|U|0\rangle \neq 0$,
2. the selected inverter $I_0 = \sum_{0 \leq i < N} (-1)^{i=0} |i\rangle\langle i| = I - 2|0\rangle\langle 0|$, and
3. the selected inverter $I_w = I - 2|w\rangle\langle w|$.

(Here, the formula $i = 0$ in the exponent stands for its numerical truth value—1 for true, 0 for false.) These combine to form *Grover's iterate*

$$G = -UI_0U^{-1}I_w. \quad (3)$$

By adjusting U by an appropriate phase factor, we can assume that $\langle w|U|0\rangle = x$ for some real $x > 0$. This adjustment leaves G unchanged.

Suppose f is as above with w unique such that $f(w) = 1$. The algorithm starts in the state $|0\rangle$ (all qubits cleared), then U is applied to get the state

$$|\psi\rangle = U|0\rangle. \quad (4)$$

Next, G is applied repeatedly to $|\psi\rangle$, approximately $\lceil \frac{\pi}{4x} \rceil$ times. At this point, the system will be very close to the state $|w\rangle$, so when we now measure the qubits we get w with high probability. Note that

$$I_w = \sum_i (-1)^{f(i)} |i\rangle\langle i|,$$

so I_w can be simulated easily given access to f alone and some extra work qubits.

In Grover's original presentation, $U = U^{-1}$ is the Walsh-Hadamard transform on n qubits, and so

$$|\psi\rangle = 2^{-n/2} \sum_i |i\rangle,$$

whence, $x = \langle w|\psi\rangle = 2^{-n/2}$, which yields the quadratic speed-up in the search.

3 Quantum Search Revisited

The point of this section is to show how one might stumble upon Grover's algorithm by taking a simplistic, almost naive, approach to quantum search. The intuition here is not geometric, as it is with Jozsa [8]; rather, it is purely algorithmic in flavor.

We start with the basic observation that if A is a skew hermitian operator ($A^\dagger = -A$) and $0 < \epsilon \ll 1$, then $I + \epsilon A$ approximates $e^{\epsilon A}$, which is unitary. Therefore, $I + \epsilon A$ approximates a plausible step in a quantum computation. By (2), we can approximate the action of e^A on a state

by repeatedly applying $I + \epsilon A$ to the state roughly $1/\epsilon$ times. The smaller ϵ is, the better the approximation. (In general, it is not certain that $e^{\epsilon A}$ is renderable by a small quantum circuit; it will be in the present case, though.)

A simple example is when $A = |i\rangle\langle j| - |j\rangle\langle i|$ for some $i, j \in \{0, 1\}^n$, $i \neq j$. Applying $I + \epsilon A$ to a state $|\varphi\rangle = \sum_i \alpha_i |i\rangle$ gives

$$(I + \epsilon A) |\varphi\rangle = |\varphi\rangle + \epsilon \alpha_j |i\rangle - \epsilon \alpha_i |j\rangle.$$

The operator alters $|\varphi\rangle$ (viewed as a column vector) by adding an ϵ fraction of its j th component into its i th component, and in exchange, subtracting an ϵ fraction of its i th component from its j th component. In a sense, we are moving probability amplitude from state $|j\rangle$ to state $|i\rangle$. With arbitrary A , this swap may take place between many pairs of components of $|\varphi\rangle$ at once.

Suppose we are given n , N , f , and w as in Section 2.1. We start in the state $|\psi\rangle = N^{-1/2} \sum_i |i\rangle$, which we would like to transform to the target state $|w\rangle$. A promising way to do this, given our considerations above, is to pile positive probability amplitude onto $|w\rangle$ while taking it away from all the other states evenly. The real skew symmetric operator that does this is

$$A = \begin{bmatrix} 0 & \dots & 0 & -1 & 0 & \dots & 0 \\ \vdots & & \vdots & \vdots & \vdots & & \vdots \\ 0 & \dots & 0 & -1 & 0 & \dots & 0 \\ 1 & \dots & 1 & 0 & 1 & \dots & 1 \\ 0 & \dots & 0 & -1 & 0 & \dots & 0 \\ \vdots & & \vdots & \vdots & \vdots & & \vdots \\ 0 & \dots & 0 & -1 & 0 & \dots & 0 \end{bmatrix}$$

expressed in the $\{|i\rangle\}$ basis, where the nonzero entries are all in the w th row and w th column. We see that

$$I + \epsilon A = \begin{bmatrix} 1 & \dots & 0 & -\epsilon & 0 & \dots & 0 \\ \vdots & & \vdots & \vdots & \vdots & & \vdots \\ 0 & \dots & 1 & -\epsilon & 0 & \dots & 0 \\ \epsilon & \dots & \epsilon & 1 & \epsilon & \dots & \epsilon \\ 0 & \dots & 0 & -\epsilon & 1 & \dots & 0 \\ \vdots & & \vdots & \vdots & \vdots & & \vdots \\ 0 & \dots & 0 & -\epsilon & 0 & \dots & 1 \end{bmatrix}.$$

The ϵ 's on row w have the effect of giving probability amplitude to $|w\rangle$ while removing it from all the other states evenly (the column of $-\epsilon$'s). The probability amplitude of $|w\rangle$ gains at the expense of an ϵ fraction of all the other probability amplitudes. From this it is clear that if we start in state $|\psi\rangle$, where all the probability amplitudes are equal, and apply $I + \epsilon A$ (for some small ϵ) the right number of times, eventually the state $|w\rangle$ will dominate.

We note that, using bracket notation,

$$A = \sqrt{N}(|w\rangle\langle\psi| - |\psi\rangle\langle w|).$$

The operator $i\epsilon A$ acts as a Hamiltonian for the time evolution of the system from $|\psi\rangle$ to $|w\rangle$. As we'll see in the next section, for the right value of ϵ , $e^{\epsilon A}$ is exactly two applications of Grover's iterate.

4 Hamiltonians

In this section, we give a Hamiltonian for Grover’s algorithm, that is, an operator H such that e^{-iHt} follows the course of the algorithm as t increases. It is clear both by geometric considerations and by the last section that such an operator must exist. H is analogous to a previous Hamiltonian H' for quantum search found by Farhi & Gutmann [3] which does not match Grover’s algorithm. We first briefly describe their results, then describe our Hamiltonian using their framework.

4.1 Farhi & Gutmann’s Hamiltonian

We are given n , N , f and w as above. Farhi & Gutmann [3] describe a physical, analog way to do quantum search by first assuming that a Hamiltonian

$$H_w = E |w\rangle\langle w|$$

is available that distinguishes the target state $|w\rangle$ from all others by giving it some positive energy E (the other basis states have energy 0). Let $|\sigma\rangle$ be some arbitrary unit vector in the Hilbert space (the “start” state). We assume $|\sigma\rangle$ is easy to prepare, so for example, $|\sigma\rangle$ may be $|\psi\rangle$ of equation (4). The goal is to evolve from $|\sigma\rangle$ into $|w\rangle$. To search for the state $|w\rangle$, we are allowed to add some “driver” Hamiltonian H_D to H_w , provided that H_D does not depend on the actual value of w at all. They choose $H_D = E |\sigma\rangle\langle\sigma|$, so their Hamiltonian is

$$H' = H_D + H_w = E (|\sigma\rangle\langle\sigma| + |w\rangle\langle w|),$$

where E is some arbitrary positive value in units of energy. If $|\sigma\rangle$ and $|w\rangle$ are not orthogonal, then we can assume as before that $\langle\sigma|w\rangle = \langle w|\sigma\rangle = x$ for some $x > 0$ by adjusting $|\sigma\rangle$ by an appropriate phase factor.

Applying $e^{-iH't}$ to the start state $|\sigma\rangle$ gives the time-evolution of the system,¹ which stays in the two-dimensional subspace spanned by $|\sigma\rangle$ and $|w\rangle$. Restricting our attention to this subspace, it is easy to see that H' has eigenvalues $E(1 \pm x)$ with corresponding eigenvectors

$$\begin{aligned} |+\rangle &= (2 + 2x)^{-1/2}(|\sigma\rangle + |w\rangle), \\ |-\rangle &= (2 - 2x)^{-1/2}(|\sigma\rangle - |w\rangle). \end{aligned}$$

A straightforward calculation yields

$$e^{-iH't} |\sigma\rangle = e^{-iEt} [\cos(xEt) |\sigma\rangle - i \sin(xEt) |w\rangle]. \quad (5)$$

When $t = \pi/(2Ex)$, we have

$$e^{-iH't} |\sigma\rangle = -ie^{-i\pi/(2x)} |w\rangle$$

as desired.

Farhi & Gutmann observe that if the unit vector $|\sigma\rangle$ is chosen at random, then the expected value of x is $N^{-1/2}$, making $t = O(N^{1/2}/E)$. For constant E , this time is the same order of magnitude as Grover’s algorithm. They show that their time evolution is optimal up to an order of magnitude for any w -independent driver Hamiltonian H_D , even one that varies with time.

¹The evolution of a quantum system under a time-independent Hamiltonian H is actually $e^{-iHt/\hbar}$. We choose units so that $\hbar = 1$, and so Et is a unitless quantity.

4.2 Another Hamiltonian

The time evolution of the system according to H' strays far from the intermediate steps Grover's algorithm. There surely is a Hamiltonian, however, whose time evolution matches the steps of Grover's algorithm exactly, since each step of Grover's algorithm essentially amounts to a rotation in a two-dimensional space. We show that this Hamiltonian can be described very simply: the operator $i\epsilon A$ mentioned at the end of Section 3 is exactly the Hamiltonian in question, for an appropriate value of ϵ which we will calculate.

The fact that Grover's iterate can be rendered by a small quantum circuit then tells us that our intuition of Section 3 is justified: the incremental application of $I + \epsilon A$ indeed corresponds to a legitimate quantum algorithm.

Given $n, N, f, |w\rangle, |\sigma\rangle, H_w$ and H_D as above, with $\langle w|\sigma\rangle = x > 0$, we define the Hamiltonian

$$H = \frac{2i}{E} [H_w, H_D] = 2iEx(|w\rangle\langle\sigma| - |\sigma\rangle\langle w|).$$

The rest of this section is devoted to proving the following

Theorem 1 *Assume the special case where $|\sigma\rangle = |\psi\rangle$ and $E = 1$. Restricted to the $(|\sigma\rangle, |w\rangle)$ -plane, e^{-iH} approximates Grover's iterate G to within $O(N^{3/2})$ in norm. In fact, e^{-iHt_0} exactly matches G where*

$$t_0 = \frac{\pi - 2 \arccos x}{2x\sqrt{1-x^2}}. \quad (6)$$

On the whole Hilbert space, e^{-2iH} approximates G^2 to within $O(N^{-3/2})$, and $e^{-2iHt_0} = G^2$.

For the moment, we allow E to be any positive value and $|\sigma\rangle$ an arbitrary unit vector with $0 < \langle w|\sigma\rangle = x < 1$. Restricting our attention to the subspace spanned by $|\sigma\rangle$ and $|w\rangle$, and letting $\theta = \arccos x$, the eigenvalues of H are seen to be $\pm \frac{1}{2}E \sin 2\theta$ with corresponding eigenvectors

$$|\pm\rangle = \frac{1}{\sqrt{2} \sin \theta} (e^{\pm i\theta} |\sigma\rangle - |w\rangle).$$

Setting $\eta = E \sin 2\theta = 2Ex \sin \theta$, a routine calculation shows that

$$e^{-iHt} |\sigma\rangle = \frac{1}{\sin \theta} [\sin(\theta - \eta t) |\sigma\rangle + \sin(\eta t) |w\rangle], \quad (7)$$

$$e^{-iHt} |w\rangle = \frac{1}{\sin \theta} [-\sin(\eta t) |\sigma\rangle + \sin(\theta + \eta t) |w\rangle]. \quad (8)$$

If x is small, θ will be close to $\pi/2$. For $t = \theta/\eta = \theta/(E \sin 2\theta) \doteq \pi/(2Ex)$ we have $e^{-iHt} |\sigma\rangle = |w\rangle$. That is, the system finds the target state in roughly the same time as with H' .

Comparing (5) and (7), we see that the quantum system evolves significantly differently under the two Hamiltonians H' and H —by more than just a global phase factor. We now show how the latter evolution, run for a short time interval, matches a single step of Grover's algorithm (one application of G). We now assume $E = 1$ and $|\sigma\rangle = |\psi\rangle = U|0\rangle$ given by equation (4), with G given by (3). We again set $x = \langle\sigma|w\rangle = \langle\psi|w\rangle = \cos \theta > 0$, for some $0 < \theta < \pi/2$.

We can express G in the basis $|\sigma\rangle, |w\rangle$:

$$\begin{aligned} G &= -U(I - 2|0\rangle\langle 0|)U^{-1}(I - 2|w\rangle\langle w|) \\ &= -(I - 2U|0\rangle\langle 0|U^\dagger)(I - 2|w\rangle\langle w|) \\ &= -(I - 2|\sigma\rangle\langle\sigma|)(I - 2|w\rangle\langle w|) \\ &= -I + 2|\sigma\rangle\langle\sigma| + 2|w\rangle\langle w| - 4x|\sigma\rangle\langle w|, \end{aligned}$$

whence

$$\begin{aligned} G|\sigma\rangle &= (1 - 4x^2)|\sigma\rangle + 2x|w\rangle, \\ G|w\rangle &= -2x|\sigma\rangle + |w\rangle. \end{aligned}$$

In view of (7), we solve the equation

$$\frac{\sin(\eta t)}{\sin \theta} = 2x = 2 \cos \theta$$

for t to get the solution

$$t_0 = \frac{\pi - 2\theta}{\eta} = \frac{\pi - 2\theta}{\sin 2\theta} = \frac{\pi - 2 \arccos x}{2x\sqrt{1-x^2}}, \quad (9)$$

as in (6). It is then easy to check that $e^{-iHt_0}|\sigma\rangle = G|\sigma\rangle$ and that $e^{-iHt_0}|w\rangle = G|w\rangle$.

Let S be the subspace spanned by $|\sigma\rangle$ and $|w\rangle$ and let S^\perp be its orthogonal complement. Let P be the orthogonal projection onto S^\perp . We have just shown that $e^{-iHt_0} = G$ restricted to S . For $|\alpha\rangle \in S^\perp$, clearly $G|\alpha\rangle = -|\alpha\rangle$, while e^{-iHt_0} leaves S^\perp pointwise fixed. Thus,

$$e^{-iHt_0} = G + 2P,$$

and since $GP = PG = -P = -P^2$, we have $e^{-2iHt_0} = G^2$ as expected.

Remark. By adding $\frac{\pi}{t_0}P$ to H , we get a slightly more complicated Hamiltonian \tilde{H} such that $e^{-i\tilde{H}t_0} = G$ on the whole Hilbert space.

Finally, we show how close t_0 is to 1, assuming $x \ll 1$. Expanding t_0 as a power series in x , we get

$$t_0 = 1 + \frac{2}{3}x^2 + O(x^4),$$

and thus

$$\begin{aligned} \left| e^{-iHt_0} - e^{-iH} \right| &= \left| e^{-iH(2x^2/3 + O(x^4))} - I \right| \\ &= \left| -\frac{2}{3}iHx^2 + O(x^4)H \right| \\ &= \frac{2}{3}x^3\sqrt{1-x^2} + O(x^5) \\ &= \frac{2}{3}x^3 + O(x^5). \end{aligned}$$

The second equation comes from expanding the exponential as a power series. The third equation holds because $|H| = |\frac{1}{2}\sin 2\theta| = x\sqrt{1-x^2}$. When $x = N^{-1/2}$, we see that e^{-iH} comes within $O(N^{-3/2})$ of $G + 2P$ in norm, and thus e^{-2iH} comes within $O(N^{-3/2})$ of G^2 .

Corollary 2 *If $t = \frac{\pi}{4}N^{1/2}$ then $e^{-iHt}|\sigma\rangle = |w\rangle + O(1/N)$.*

4.3 Discussion

Farhi and Gutmann show that the Hamiltonian H' finds the target in optimal time in the following sense: no other Hamiltonian of the same form—that is, $H_D + E |w\rangle\langle w|$ where H_D has no special dependence on w —can find $|w\rangle$ any faster, even if H_D is allowed to depend on time. Our Hamiltonian is clearly not of this form, so their lower bounds aren't directly applicable here. Indeed, it is only by the lower bounds shown for “digital” quantum search [1] that we know that our Hamiltonian is optimal to simulate a small digital quantum circuit. It is an interesting question whether one can deduce the same lower bound by more direct means.

5 Further Research and Open Problems

We have seen how Grover's algorithm can be described much more simply using a Hamiltonian than directly with unitary operators. We don't present details them here, but variants of Grover's original algorithm also admit simple Hamiltonian descriptions. There may be new, yet unknown quantum algorithms which are more easily described with Hamiltonians than with unitary operators, and which may indeed be first discovered by their Hamiltonians.

There are two principal challenges to fashioning a new quantum algorithm via a Hamiltonian:

1. finding an appropriate, and hopefully intuitive, Hamiltonian for the problem at hand, and
2. deciding how (or if) the time evolution governed by such a Hamiltonian approximates a true (digital) quantum algorithm given by a small quantum circuit.

In the case of Grover's algorithm considered here, we were fortunate to achieve both goals. Grover's algorithm came first, however, so we knew what to shoot for. Even so, the intuition provided in Section 3 may be useful for constructing new algorithms, or at least viewing other existing algorithms from a different angle.

Our results thus point to an important general question: when, given a Hamiltonian on a system of qubits, can the corresponding time evolution be simulated (even approximately) by a small quantum circuit? Is there an easy criterion, based on the structure of the Hamiltonian itself? Such a criterion would provide a new way to prototype new quantum algorithms via Hamiltonians.

Can Farhi & Gutmann's original H' be simulated efficiently by a quantum circuit?

Recently, Farhi, *et al.* [2] show how to solve certain instances of SAT with slowly time-dependent Hamiltonians (adiabatic evolution). Their results provide good physical intuition. Is there a corresponding algorithmic intuition?

Can one find an intuitive Hamiltonian for a quantum factoring algorithm?

6 Acknowledgments

I would like to thank Frederic Green and Steven Homer for helpful discussions.

References

- [1] C. H. Bennett, E. Bernstein, G. Brassard, and U. Vazirani. Strengths and weaknesses of quantum computation. *SIAM J. Comp.*, 26(5):1510–1523, 1997, quant-ph/9701001.
- [2] E. Farhi, J. Goldstone, S. Gutmann, and M. Sipser. Quantum computation by adiabatic evolution, 2000, quant-ph/0001106. MIT CTP #2936.

- [3] E. Farhi and S. Gutmann. An analog analogue of a digital quantum computation. *Physical Review A*, 57:2403–2406, 1998, quant-ph/9612026. MIT CTP #2593.
- [4] L. K. Grover. A fast quantum mechanical algorithm for database search. *Physical Review Letters*, 78:325, 1997, quant-ph/9605043.
- [5] L. K. Grover. A framework for fast quantum mechanical algorithms. In *Proceedings of the 30th ACM Symposium on the Theory of Computing*, pages 53–62, 1998, quant-ph/9711043.
- [6] L. K. Grover. Quantum computers can search rapidly by using almost any transformation. *Physical Review Letters*, 80:4329–4332, 1998, quant-ph/9712011.
- [7] J. Gruska. *Quantum Computing*. McGraw-Hill, 1999.
- [8] R. Jozsa. Searching in Grover’s algorithm, 1999, quant-ph/9901021.
- [9] P. W. Shor. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM Journal on Computing*, 26:1484–1509, 1997, quant-ph/9508027.